Deutscher Bundestag **Drucksache 18/2674**

18. Wahlperiode 26.09.2014

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Annette Groth, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/2505 –

Die neue „Joint Cybercrime Action Taskforce“ bei Europol

Vorbemerkung der Fragesteller

Das Europäische Polizeiamt (Europol) hat am 1. September 2014 seine „Joint Cybercrime Action Taskforce“ (J-CAT) in Betrieb genommen (Pressemitteilung Europol vom 1. September 2014). Die Einheit ist in Den Haag angesiedelt. Dort hatte Europol bereits vor zwei Jahren das European Cybercrime Center (EC3) eingerichtet. Laut einer Mitteilung des Bundeskriminalamtes (BKA) vom 1. September 2014 haben Behörden aus Deutschland, Frankreich, Italien, Spanien, Großbritannien, den Niederlanden und Österreich „Cybercrime-Experten“ entsandt. Demnach seien auch „Cybercrimedienststellen“ aus den USA, Kanada, Australien und Kolumbien an der Initiative beteiligt. Auch die Privatwirtschaft sei eingebunden.

Die Einrichtung der „Joint Cybercrime Action Taskforce“ wird mit „gestiegenen Herausforderungen bei der Bekämpfung der Computer- und Internetkriminalität“ begründet. Das BKA hatte hierzu im September 2014 ein „Bundeslagebild Cybercrime 2013“ veröffentlicht. Es ist aus Sicht der Fragesteller fraglich, wozu die neue „Joint Cybercrime Action Taskforce“ überhaupt notwendig ist: Europol kann bei Bedarf sogenannte Gemeinsame Ermittlungsteams einrichten. Hiervon wird auch im Bereich der Internetkriminalität rege Gebrauch gemacht. Mehrere Mitgliedstaaten der Europäischen Union (EU), darunter auch Deutschland, beteiligten sich unter Mitarbeit von Europol an Razzien gegen vermeintliche Mitglieder des Anonymous-Netzwerks. Die weltweite Aktion wurde zusammen mit der Internationalen kriminalpolizeilichen Organisation (Interpol) ausgeführt (Pressemitteilung Europol vom 28. Februar 2012). Europol richtete damals ein internationales Treffen zu „Hacktivismus“ aus, um Ermittlungsverfahren zu koordinieren und das weitere Vorgehen zu planen.

Vorbemerkung der Bundesregierung

Am 1. September 2014 haben das Europäische Polizeiamt Europol, das Bundeskriminalamt (BKA) und andere internationale Experten zur Bekämpfung von Cybercrime die Arbeit in der Joint Cybercrime Action Taskforce (J-CAT) in Den Haag/Niederlande aufgenommen. Initiiert wurde die J-CAT durch das European

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 24. September 2014 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Cybercrime Center (EC3) bei Europol. Neben Deutschland beteiligen sich weitere europäische Staaten, darunter Frankreich, Italien, Spanien, Großbritannien, die Niederlande und Österreich sowie Cybercrimedienststellen aus den USA, Kanada, Australien und Kolumbien an der Initiative. Das BKA reagiert mit seiner Beteiligung am J-CAT und der Entsendung eines Cybercrime-Experten auf die gestiegenen Herausforderungen bei der Bekämpfung von Computer- und Internetkriminalität. Die Joint Cybercrime Action Taskforce bei Europol ermöglicht die Intensivierung der internationalen Zusammenarbeit bei der Bekämpfung von Cybercrime. Sie ist somit ein weiterer Baustein für die zeitgemäße Bekämpfung der Cybercrime im internationalen Verbund.

In den Antworten zu den Fragen 24 und 25 sind Auskünfte enthalten, die unter dem Aspekt des Schutzes der nachrichtendienstlichen Zusammenarbeit mit ausländischen Partnern besonders schutzbedürftig sind. Eine öffentliche Bekanntgabe von Informationen zu technischen Fähigkeiten von ausländischen Partnerdiensten und damit einhergehend die Kenntnisnahme durch Unbefugte würde erhebliche nachteilige Auswirkungen auf die vertrauensvolle Zusammenarbeit haben. Würden in der Konsequenz eines Vertrauensverlustes Informationen von ausländischen Stellen entfallen oder wesentlich zurückgehen, entstünden signifikante Informationslücken mit negativen Folgewirkungen für die Genauigkeit der Abbildung der Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland. Die künftige Aufgabenerfüllung der Nachrichtendienste des Bundes würde stark beeinträchtigt. Insofern könnte die Offenlegung der entsprechenden Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die Antworten zu den genannten Fragen teilweise als Verschlusssache gemäß der VSA mit dem Geheimhaltungsgrad „VS – Geheim“ eingestuft.

1. Inwiefern hat sich die Bundesregierung am Zustandekommen der „Joint Cybercrime Action Taskforce“ beteiligt?

Das BKA war im Rahmen von drei Workshops bei Europol in die Vorbereitung der „Joint Cybercrime Action Taskforce“ eingebunden.

2. Wie hat sich die deutsche Delegation hierzu in den zuständigen Ratsarbeitsgruppen positioniert, und welche Fragen waren diesbezüglich strittig?

Das Zustandekommen der „Joint Cybercrime Action Task Force“ wurde in einschlägigen Ratsgremien nicht behandelt.

3. Worin liegt aus Sicht der Bundesregierung der Mehrwert gegenüber bereits existierenden Zusammenarbeitsformen mit Europol?

Durch das Einrichten dieser Task Force soll die gemeinsame, grenzüberschreitende Zusammenarbeit in relevanten und in der Regel mehrere Staaten betreffenden Cybercrime-Sachverhalten bzw. Ermittlungsverfahren beschleunigt und intensiviert werden. Durch Zusammenführen der Vertreter von Sicherheits- bzw. Strafverfolgungsbehörden der teilnehmenden Länder bei Europol werden internationale Kommunikationsprozesse verkürzt und insgesamt die Zusammenarbeit zwischen den jeweiligen Behörden und Europol somit verbessert und vereinfacht. Mehrwert ist durch die hier organisierte Einbindung der Nicht-EU-Mitgliedstaaten zu erwarten.

4. Welche privaten Firmen oder Institute sind nach Kenntnis der Bundesregierung an der „Joint Cybercrime Action Taskforce“ beteiligt, und worin besteht deren Mitarbeit?

An der Task Force sind keine privaten Firmen oder Institute beteiligt. Informationen oder Daten privater Firmen oder Institute wären im Rahmen der jeweiligen rechtlichen Bestimmungen bedarfs- oder anlassbezogen über Europol oder die zuständigen Stellen der Teilnehmenden Länder einzubeziehen.

5. Welche Behörden sind nach Kenntnis der Bundesregierung aus Frankreich, Italien, Spanien, Großbritannien, den Niederlanden und Österreich an der „Joint Cybercrime Action Taskforce“ beteiligt?

Nach Kenntnis der Bundesregierung sind die genannten Länder mit Teilnehmern der Guardia Civil, Policia Nacional (Spanien), Police Nationale (Frankreich), Bundeministerium des Innern (Österreich), National Crime Agency (Großbritannien), National High Tech Crime Unit (Niederlande) und der Polizia di Stato (Italien) vertreten.

6. Welche „Cybercrimedienststellen“ sind nach Kenntnis der Bundesregierung aus den USA, Kanada, Australien und Kolumbien an „Joint Cybercrime Action Taskforce“ beteiligt?

Nach Kenntnis der Bundesregierung sind aus den USA das FBI und der US Secret Service vertreten. Kanada kooperiert über das bei Europol ansässige Verbindungsbüro mit J-CAT. Die Entsendung der Vertreter Australiens und Kolumbiens steht noch bevor, zu den entsendenden Dienststellen dieser Länder liegen der Bundesregierung derzeit keine Informationen vor.

7. Worin besteht aus Sicht der Bundesregierung der Mehrwert ihrer Teilnahme?

Cybercrime ist ein weltweites und grenzüberschreitendes Problem, bei dem die beteiligten Länder, insbesondere die USA, eine wichtige Rolle einnehmen. Eine effektive Bekämpfung von Cybercrime wird aufgrund der zahlreichen US-Diensteanbieter im Bereich der Infrastruktur durch Beteiligung von Vertretern der Cybercrimedienststellen der USA deutlich verbessert.

8. Welche Aufgaben sollen diese „Cybercrimedienststellen“ aus den USA, Kanada, Australien und Kolumbien nach Kenntnis der Bundesregierung in der „Joint Cybercrime Action Taskforce“ übernehmen?

Die genannten Cybercrime-Dienststellen sollen den Informations- und Wissensaustausch in die betreffenden Länder bei internationalen Bezügen gewährleisten.

9. Wie sollen diese „Cybercrimedienststellen“ aus den USA, Kanada, Australien und Kolumbien in der „Joint Cybercrime Action Taskforce“ nach Kenntnis der Bundesregierung administrativ und organisatorisch eingebunden werden, und an welchen Treffen werden diese teilnehmen?

Die vor Ort befindlichen Vertreter der genannten Staaten sollen in der Task Force gleichberechtigt mitarbeiten. Dabei wird die jeweilige Einbindung und Beteiligung von der zugrunde liegenden Fallgestaltung abhängig sein.

10. Welche Kriminalitätsphänomene sollen nach Kenntnis der Bundesregierung von der „Joint Cybercrime Action Taskforce“ konkret verfolgt werden?

Nach derzeitiger Planung sollen Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten, verfolgt werden.

11. Auf welche Weise wird sich die „Joint Cybercrime Action Taskforce“ nach Kenntnis der Bundesregierung mit Hackerangriffen und dem Netzwerk TOR befassen?

Die J-CAT wird sich bedarfs- und anlassbezogen mit als relevant eingeschätzten Bedrohungslagen und Sachverhalten aus dem Bereich der Cybercrime befassen. Über die spezifische Art und Weise einer zukünftigen Befassung der J-CAT mit konkreten Themen wie Hackerangriffen und dem TOR-Netzwerk liegen der Bundesregierung derzeit keine Kenntnisse vor.

12. Inwiefern hält die Bundesregierung TOR für ein brauchbares Werkzeug zur Aufrechterhaltung der digitalen Privatsphäre?

Die Bundesregierung befürwortet Maßnahmen, die der Verbesserung von Datenschutz und Datensicherheit dienen. Hierzu zählen insbesondere auch Technologien, Verfahren und Anwendungen, die dem Schutz personenbezogener oder vertraulicher Daten vor unbefugten Zugriffen Dritter einschließlich der Anonymisierung und Pseudonymisierung dienen. Dies entspricht auch dem Grundgedanken des Telemedienrechts. Nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist TOR für niedrigen bis mittleren Schutzbedarf ein brauchbares Werkzeug zur Aufrechterhaltung der digitalen Privatsphäre.

13. Auf welche Weise wird das BKA mit der „Joint Cybercrime Action Taskforce“ kooperieren?

Das BKA entsendet einen Mitarbeiter für die sechsmonatige Pilotphase von J-CAT.

14. In welcher Dienststelle ist der entsandte „Cybercrime-Experte“ angesiedelt?

Der vom BKA entsandte Mitarbeiter ist im BKA bei der Fachdienststelle „Auswertung Cybercrime“ angesiedelt.

15. Inwiefern und auf welche Weise soll die „Joint Cybercrime Action Taskforce“ nach Kenntnis der Bundesregierung Bedrohungen bereits im Vorfeld analysieren?

Grundsätzliches Ziel der J-CAT ist es, auf Grundlage von Auswertung koordinierte Maßnahmen gegen Hauptakteure und Erscheinungsformen aus dem Phänomenbereich Cybercrime zu betreiben, indem Ermittlungsverfahren auf nationaler Ebene eingeleitet werden.

16. Auf welche Weise werden hierzu nach Kenntnis der Bundesregierung Informationen aus „offenen Quellen“ gespeichert und verarbeitet?

Es gelten die bisherigen Regelungen: Die Mitgliedstaaten und Europol erfassen Informationen und tauschen diese im Rahmen der rechtlichen Befugnisse aus, für Deutschland auf Grundlage des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG), für Europol insbesondere auf Grundlage des Ratsbeschlusses 2009/371/JI vom 6. April 2009 zur Errichtung des Europäischen Polizeiamtes (Europol). Die J-CAT verfügt hierzu über keine zusätzlichen Befugnisse.

17. Auf welche Weise und in welchen Fällen werden hierzu nach Kenntnis der Bundesregierung Informationen aus polizeilichen Informationssystemen gespeichert und verarbeitet?

Der Informationsaustausch zwischen den J-CAT-Teilnehmern wird innerhalb des bisher üblichen rechtlichen Rahmens für den internationalen polizeilichen Informationsaustausch erfolgen. Auf die Antwort zu Frage 16 wird verwiesen.

18. Welche Datensammlungen wurden nach Kenntnis der Bundesregierung für die Arbeit der „Joint Cybercrime Action Taskforce“ eingerichtet?

Die Task Force greift auf die bei Europol vorliegenden Informations- und Auswertemöglichkeiten zurück.

19. Auf welche „Focal Points“ kann die „Joint Cybercrime Action Taskforce“ nach Kenntnis der Bundesregierung zugreifen?

Die J-CAT wird bedarfs- bzw. anlassbezogen mit Vertretern der Focal Points „Cyborg“, „Terminal“ und „Twins“ zusammenarbeiten.

20. Was ist der Bundesregierung über Hintergründe einer Forderung der Innenminister der Länder zur Schaffung einer „Zentralstelle für die Verfolgung von Internetkriminalität“ bei den Staatsanwaltschaften bekannt, und wie wird sie sich hierzu positionieren (Pressemitteilung des Ministeriums für Inneres und Sport des Landes Mecklenburg-Vorpommern vom 5. September 2014)?

In der Konferenz der Innenminister und -senatoren der Union (B-IMK) am 4. und 5. September 2014 wurde durch den thüringischen Innenminister Geibert die Schaffung einer Zentralstelle für die Verfolgung von Internetkriminalität bei den Staatsanwaltschaften angeregt; eine Beschlussfassung erfolgte hierzu nicht.

21. Auf welche Weise befassen sich das BKA und Europol nach Kenntnis der Bundesregierung derzeit mit dem Phänomen „Hacktivismus“ und der Repression vermeintlicher Mitglieder des Anonymous-Netzwerks?

Das BKA führt seit dem 2. Januar 2013 ein Forschungsprojekt mit dem Ziel durch, Hacktivismus phänomenologisch zu beschreiben und von verwandten Cybercrime-Bereichen abzugrenzen. Über entsprechende Aktivitäten der Europol liegen der Bundesregierung keine Erkenntnisse vor.

22. Welche Mitteilungen haben Bundesbehörden im Rahmen von Ermittlungen bzw. der Anklageerhebung gegen den Gründer der Filesharing-Website Pirate Bay, Gottfrid Svartholm Warg, gegenüber dänischen Behörden gemacht, der für das Eindringen in das Schengen-Informationssystem verantwortlich gemacht wird, dies aber vehement bestreitet (www.heise.de vom 2. September 2014)?

Seitens Bundesbehörden erfolgten keine Mitteilungen im Rahmen von Ermittlungen bzw. der Anklageerhebung gegen den Gründer der Filesharing-Website Pirate Bay, Gottfrid Svartholm Warg, gegenüber dänischen Behörden.

23. Welche neueren Erkenntnisse hat die Bundesregierung darüber, ob bzw. wo es bis heute einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat (Bundestagsdrucksachen 17/7578 und 18/164)?

Der Bundesregierung liegen keine neueren Erkenntnisse zu versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlägen“ vor. Auf die Antwort der Bundesregierung zu Frage 43 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/164 vom 12. Dezember 2013 wird verwiesen.

24. Welche Angriffe auf digitale Infrastrukturen der Bundesregierung hat es im Jahr 2013 gegeben, die nachweislich bzw. mit großer Wahrscheinlichkeit von ausländischen Nachrichtendiensten begangen wurden, um welche Angriffe bzw. Urheber handelt es sich dabei, und in wie vielen Fällen wurde Schadsoftware mittels mobiler Datenträger in die IT-Netze eingebracht?

Täglich werden mehrere E-Mails mit Anhängen von Schadsoftware an den besonders gesicherten Übergängen vom Internet zum Regierungskommunikationsnetz (IVBB) detektiert, die vor dem Hintergrund einer Beurteilung ihrer Qualität sowie ihrer Anhänge mit hoher Wahrscheinlichkeit einen nachrichtendienstlichen Urheber vermuten lassen. Es kann bei solchen hochqualifizierten E-Mails mit Schadsoftwareanhängen regelmäßig nicht zweifelsfrei nachgewiesen werden, wer jeweils Initiator solcher Schad- und Spionageprogramme war oder ist. Sofern der Verdacht besteht, dass Schadsoftware insbesondere über mobile Datenträger wie bspw. USB-Sticks eingebracht wurde, werden bspw. im Zusammenwirken zwischen dem betroffenen Ressort und dem BSI entsprechende Maßnahmen getroffen.

Zu weiteren Details wird hierzu auf den eingestuften Bericht des BSI gemäß § 5 Absatz 9 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) an den Deutschen Bundestag verwiesen, der jährlich im Innenausschuss vorgestellt wird. Zudem wird auf die Vorbemerkung der Bundesregierung verwiesen.*

25. Welche Angriffe auf digitale Infrastrukturen der Bundesregierung hat es im Jahr 2013 gegeben, die vermutlich von ausländischen Nachrichtendiensten begangen wurden, um welche Angriffe bzw. Urheber handelt es sich dabei, und in wie vielen Fällen wurde Schadsoftware mittels mobiler Datenträger in die IT-Netze eingebracht?

Auf die Antwort zu Frage 24 wird verwiesen.*

* Das Bundesministerium des Innern hat die Teile der Antwort als „VS – Geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

26. Welche Treffen der „Friends of the Presidency Group on Cyber Issues“ haben nach Kenntnis der Bundesregierung auf EU-Ebene im Jahr 2014 stattgefunden, wer nahm daran jeweils teil, und welche Tagesordnung wurde behandelt?

In der Ratsformation „Friends of the Presidency Group on Cyber Issues“ werden mit dem Ziel, eine bessere Koordinierung innerhalb der EU zu erreichen, übergreifend Fragen der Cyber-Politik der EU behandelt. Innerhalb der Bundesregierung liegt die gemeinsame Federführung bei Auswärtigem Amt (AA) und Bundesministerium des Innern (BMI). Es finden sowohl Treffen im Hauptstadtformat, die jeweils durch Vertreter des BMI und des AA wahrgenommen werden, als auch im Brüsseler Format, die durch Vertreter der StÄV wahrgenommen werden, statt.

Es fanden in 2014 bisher folgende Treffen statt:

– am 24. Februar 2014 und 23. Mai 2014 jeweils Treffen im Hauptstadtformat (im Treffen am 24. Februar 2014 war BMI durch einen Mitarbeiter des BSI vertreten);

– am 30. Januar 2014, 25. März 2014, 14. Mai 2014, 10. Juni 2014 und 23. Juli 2014 jeweils Treffen im Brüsseler Format.

Der erste Teil der Tagesordnung ist in der Regel eine Information seitens der amtierenden EU-Ratspräsidentschaft bzw. der Europäische Kommission und des Europäischen Auswärtigen Dienstes über aktuelle EU-Vorgänge mit digitalen Bezügen. Der zweite Teil der Tagesordnung befasst sich mit aktuell anstehenden Terminen und Konferenzen (z. B. NETmundial-Konferenz in Sao Paulo, Internet Governance Forum in Istanbul) sowie dem Umsetzungsstand von zentralen Strategiedokumenten wie bspw. der EU-Cybersicherheitsstrategie. Zudem erhalten EU-Mitgliedstaaten die Möglichkeit, nationale Initiativen vorzustellen.

27. Auf welche Weise ist der Komplex „Cybersicherheit“ nach Kenntnis der Bundesregierung im Rahmen der „Integrated Political Crisis Response“ (IPCR) der Europäischen Union berücksichtigt?

Bei einer Katastrophe oder einem Terroranschlag kann der betroffene Mitgliedstaat gemäß Artikel 4 des Beschlusses zur Anwendung der Solidaritätsklausel (ABl. EU L 192/56 vom 1. Juli 2014) die Klausel geltend machen, wenn er nach Ausschöpfung aller nationaler und auf Unionsebene vorhandenen Mittel und Instrumente der Auffassung ist, dass die Krise die ihm zur Verfügung stehenden Maßnahmen eindeutig übersteigt. Grundsätzlich können auch „Cyberkrisen“ in den Anwendungsbereich der Solidaritätsklausel fallen, wenn sie katastrophale Auswirkungen haben oder auf einem Terroranschlag beruhen. Außerdem wäre auch eine Aktivierung des EU-Katastrophenschutzverfahrens (ABl. EU L 347/924 vom 20. Dezember 2013) zur Unterstützung bei der Folgenbeseitigung denkbar, wenn durch den Ausfall von IT-Systemen gravierende Folgen auftreten sollten, die mit Mitteln des Katastrophenschutzes zu bewältigen wären.

28. Welche IPCR-Übungen sollen nach Kenntnis der Bundesregierung in den Jahren 2014 und 2015 stattfinden, wo werden diese abgehalten, und wer wird jeweils teilnehmen?

Im Jahr 2014 soll eine eintägige IPC-Übung im Zeitraum vom 27. November bis 5. Dezember 2014 stattfinden. Die konkrete Ausgestaltung der Teilnahme der

Bundesregierung befindet sich derzeit in Abstimmung zwischen dem BMI und dem AA.

Informationen über eine Übung im Jahr 2015 liegen bislang nicht vor.

29. Welche Auslöser von Krisen werden nach Kenntnis der Bundesregierung jeweils angenommen, und welche Szenarien werden jeweils durchgespielt?

Der Übung 2014 soll ein fiktives Cyber-Szenario zugrunde gelegt werden, welches sich inhaltlich an die CyberEurope 2014 anlehnt. Der konkrete Szenarienablauf wird aktuell noch von einem sogenannten Exercise Planning Team (EPT) ausgestaltet.

30. Auf welche Weise bringen sich Bundesbehörden in die Vorbereitung der Übungen ein?

Die grundsätzlichen Belange für die Übung werden in der „Friends of the Presidency Group on Cyber Issues“ zur Umsetzung der Solidaritätsklausel bearbeitet; in dieser wirken AA und BMI mit. Im in der Antwort zu Frage 29 beschriebenen EPT ist eine Mitwirkung der Bundesregierung bislang nicht vorgesehen.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333